IDAHO STATE DEPARTMENT OF AGRICULTURE	
APPROVED BY:	
ORIGINAL EFFECTIVE DATE: January 1, 2003	**REVISION DATE:**
TITLE: Employee Electronic Mail And Messaging Use Policy	

Purpose

The purpose of this policy is to ensure proper and efficient use of Idaho State Department of Agriculture's (ISDA) electronic mail and messaging systems by its employees.

I. Definitions

Electronic mail (E-mail) is any electronic communication between two or more individuals and may contain any form or combination of text, audio, video, drawings, or photographic representation. This definition includes "Instant Messenger Services and/or Chat Rooms."

A. The Internet is a network of connected sites accessible through a 'web browser' and is a resource for research, information gathering, extending and obtaining services, and education.

B. "Internet Access" includes all available routes to the Internet, including direct Internet Provider access and Modem/ISP individual accounts.

C. "Worm" refers to a program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as monopolizing the computer or network's resources and shutting systems down.

D. "Virus" means a program or piece of code that is loaded onto a computer without the users knowledge and runs against the users wishes. It may contain a self-replicating component to spread the "infection."

E. "Trojan Horse" is a destructive program that masquerades as a benign application. Unlike viruses, Trojan Horses do not replicate themselves but they can be as destructive.

II. Policy

A. Electronic mail is a tool for business communications. Users have the responsibility to use this resource in an efficient, effective, ethical, and lawful manner. E-mail communications must comply with all applicable laws, regulations and generally accepted business etiquette.

B. The primary purpose of electronic mail is to conduct official business. Employees may occasionally use the department's electronic mail for individual, nonpolitical purposes on their personal time, if such use does not violate the terms and conditions of this policy or interfere with ISDA business.

C. All E-mail accounts maintained on the E-mail systems are the sole property of ISDA. The Agency has the right to monitor any employee's E-mail account. Any unauthorized or inappropriate use discovered during such monitoring activities shall be formally reported to department management for determination of appropriate action.

D. Users should not expect their E-mail communications, documents, or other information to be private and should not use the E-mail system for matters that are not intended for public disclosure. Confidential matters, permitted by law, should be so marked and include a warning regarding accidental transmission to a third-party.

E. E-mail messages are considered ISDA property, constitute official records of ISDA, and are subject to public records law. Sending data via E-mail is the same as sending correspondence on official memo or letterhead.

F. Use of the E-mail system as described below is **strictly prohibited**. Users who receive such information should not forward or respond to it except to forward to "abuse".

1. Knowingly or intentionally creating, publishing, transmitting, and/or exchanging messages that are inappropriate, offensive, harassing, obscene, or threatening.

2. Creating or distributing E-mail containing defamatory, false, inaccurate, abusive, threatening, racially offensive or otherwise biased, discriminatory or illegal material.

3. Viewing or distributing obscene, pornographic, profane, or sexually oriented material.

4. Violating laws, rules and regulations prohibiting sexual harassment.

5. Encouraging the use of controlled substances for criminal or illegal purposes.

6. Engaging in any activities for personal gain.

7. Distributing copyrighted information without permission.

8. Distributing advertisements for commercial enterprises, including but not limited to, goods, services, or property unless such advertisements are part of requested vendor information to be used in carrying out ISDA business.

9. Violating or infringing upon the rights of others.

10. Conducting business unauthorized by the department.

11. Transmitting incendiary statements, which might incite violence or describe or promote the use of weapons.

12. Conducting any non-department supported fund raising or public relations activities.

13. Exchanging proprietary information, trade secrets, or any other privileged, confidential, or sensitive information that is not authorized.

14. Creating or exchanging solicitations, chain letters, and other unsolicited E-mail.

15. Registering to non-ISDA business related E-Mail servers without proper authorization. Subscription to such a service can result in an overload of received messages directly impacting the performance of ISDA E-mail systems.

16. Conducting political activity.

17. Using the system for any illegal purpose.

G. Users shall not knowingly or willfully create or propagate any virus, worm, Trojan Horse, or other destructive program code.

1 Individual use of the E-mail messaging systems is subject to monitoring by the respective Agency or upon request by the Agency, by authorized Department of Administration staff.

2 Violations of this policy may result in disciplinary action, up to and including dismissal.

III. Responsibility

Employees using the E-mail system are deemed to have accepted the responsibilities and obligations imposed by federal, state, and local laws and regulations as well as ITRMC and department adopted policies, procedures, standards, and guidelines.

A. Users should not pursue, obtain, exchange, or distribute any non-authorized information that could cause congestion or disruption to E-mail systems such as screen savers, audio, or video clips, or in violation of any licensing agreement.

B. Users shall not access another's E-mail system without authorization from that user or that user's supervisor.

C. Users must not compromise the privacy of their password by giving it to others or exposing it to public view. Passwords should be changed on a regular basis.

D. Users should schedule, wherever possible, communications-intensive operations such as large file transfers, video downloads, mass E-mailings, and the like for off-peak usage times.